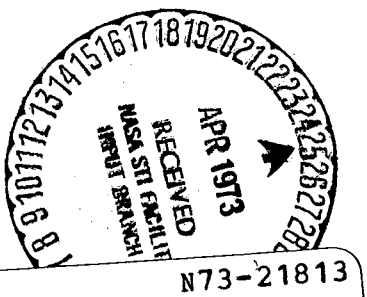
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Memorandum 33-593

Low-Thrust Mission Risk Analysis, With Application to a 1980 Rendezvous With the Comet Encke

C. L. Yen

D. B. Smith



JET PROPULSION LABORATORY

CALIFORNIA INSTITUTE OF TECHNOLOGY

PASADENA, CALIFORNIA

March 15, 1973

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Technical Memorandum 33-593

Low-Thrust Mission Risk Analysis, With Application to a 1980 Rendezvous With the Comet Encke

C. L. Yen
D. B. Smith

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

March 15, 1973

Prepared Under Contract No. NAS 7-100
National Aeronautics and Space Administration

PREFACE

The work described in this report was performed by the Mission Analysis Division of the Jet Propulsion Laboratory.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the contributions of M. McKinley of the K. M. S. Technology Center and T. A. Barber of the Jet Propulsion Laboratory for providing valuable suggestions. The generous support of C. G. Sauer in obtaining necessary trajectory information is most appreciated.

CONTENTS

CONTENTS (contd)

ABSTRACT

A computerized multistage failure process simulation procedure is used to evaluate the risk in a solar electric space mission. The procedure uses currently available thrust-subsystem reliability data and performs approximate simulations of the thrust subsystem burn operation, the system failure processes, and the retargeting operations. The method is applied to assess the risks in carrying out a 1980 rendezvous mission to the comet Encke. Analysis of the results and evaluation of the effects of various risk factors on the mission show that system component failure rates are the limiting factors in attaining a high mission reliability. It is also shown that a well-designed trajectory and system operation mode can be used effectively to partially compensate for unreliable thruster performance.

I. INTRODUCTION

One unique feature of a low-thrust system is the ability to accomplish the primary mission and/or science objectives even if one or more of its thrusters fail, so long as the solar panel power output (energy supply) remains available. This flexibility can greatly increase the probability of a mission's success, [1] if a complete scenario of alternate thrust profiles is included as part of the mission operations strategy. This avoids excessive reliance on redundant hardware or expensive improvements in hardware reliability and longevity.

Previous reliability studies, such as Refs. 1 and 2, do not consider the effects of these alternate maneuver possibilities. Further refinements and realistic risk assessment require development of analysis techniques to cope with this additional, fundamentally complex factor. Within this general context, we seek a methodology which evaluates risk with at least first order correctness and maximum practical utility.

A discrete, multistage process simulation procedure is used. Essentially, continuous and infinite processes are modeled as discrete and finite sequences. The discrete simulation approach, with finite stochastic sequences, is especially attractive for low-thrust missions since the actual flight mode will probably be operationally discrete anyway. Various thrust subsystem parameters, hardware reliability factors, and mission operation modes, which affect the process simulation and thus the assessed value of the risks, are analyzed. The results of such analyses provide guidelines for rational thrust-subsystem design and can be used to identify the key risk factors.

---

[1] The simple mission success criteria used here assume a satisfactory science return if a specified set of state conditions such as rendezvous, flyby, etc. are achieved within a desired time period.

II. MODEL OVERVIEW

The performance of a desired mission is tied to the operation of a system. To assess the risk in a mission, one must understand the proposed mission profile, the operational system, and its operational processes.

In this study, the system is a solar electric (SEP) spacecraft with attention focused on the thrust subsystem. Generally, a thrust subsystem comprises several units of power conditioners (PC) and thrusters interconnected by a switching mechanism.

In a SEP mission, since the thrust power varies with time, the number of thrusters needed to be burning at various phases of the mission must vary according to the power level. Therefore, operation of this system requires not only the steering of the spacecraft along the desired path (vector control), but also the timely switching of thrusters (thruster burn control) to match the power.

For the purpose of the risk analysis, the state of the operational system at time t, S(t), is conveniently defined in the following way:

$$S(t) = \begin{pmatrix} X \\ U \\ \tau \end{pmatrix}, \qquad U = \begin{bmatrix} U_1 \\ U_2 \\ \vdots \\ U_N \end{bmatrix} \qquad \tau = \begin{bmatrix} \tau_1 \\ \tau_2 \\ \vdots \\ \tau_N \end{bmatrix} \tag{1}$$

where U and τ are column vectors with N components, used to represent the status and elapsed burn time of the N given thrusters. Components of U are integers (2), (1) or (0) depending on whether the thruster is operating, idling, or failed, and X represents the spacecraft states (X, Y, Z, V_X, V_Y, V_Z). Propagation of the operational system state S from time t to $t + \Delta t$ is governed by the operational control policies, namely a path control policy (such as payload optimizing control, minimum mission time control, etc.) and a burn control policy. A unique, well-defined control policy must be able to transfer the state in a unique manner with 100 percent certainty. But, as in any real dynamic system, the state of the system is under the influence of uncontrollable internal and external random forces, and the

actual behavior of the controls forces the state to exhibit deviations. Thus, the state transitions from $S_i(t)$ to $S_j(t+\Delta t)$ can be described only in probabilistic terms. The sole source of random control concerned with here is the thruster failures, and this failure statistic is assumed to be given. Other small random forces such as process noise (noise in the thrust vector) are considered as insignificant for this risk analysis. Since a thruster failure destroys a large fraction of the thrust subsystem capability, the stochastic failure effects predominate in this operational system. This operational process is complex because (1) it is continuous in time, (2) the process control is time-dependent (both in deterministic control and random failure), (3) the state S(t) occupies a continuous space and, above all, (4) the random effects can be violent. This complexity indicates that an analytical approach, such as setting up differential equations for the deviations (Ref. 3), cannot be used, and this leads to a simulation procedure. Monte Carlo simulation could be used if one were to ignore the trajectory control effects on the mission and simulate only the burn control processes for a particular thrust program (Refs. 1 and 2). If one includes the trajectory aspect in this type of simulation in a straightforward manner, the trajectory computation cost becomes prohibitive.

The procedure used here is that of discretized simulation. Time is divided into stages, and X and τ are conceptually discretized at each stage time, by way of an approximate representation, as will be discussed in detail later. Since the U component of the system state S is denumerable, the state at each stage time can be counted. This procedure reduces the process to a multistage diverging network problem. For the risk analysis, the probability tree corresponding to such processes can be constructed. The propagation along all the successful paths can be computer simulated and the probability of success obtained (see Fig. 1). Nonetheless, since the tree can branch out very quickly as the stage progresses forward, a compromise must be made between the accuracy and the volume of computation.

III. RISK FACTORS

Various risk factors included in this risk assessment procedure are shown in Fig. 2. A detailed description and analysis of each of these risk factors are presented in the following sections.

A. Operational Mode Risk Factors

The impact of a failure on the mission goal depends on the time and type of failures (failure modes). Fatal failure modes can be identified by systematic trajectory error analysis. The probability of occurrence of such failure events depends not only on the nature of the hardware but also on the strategy used in operating the available thrusters (burn policy). In planning a mission, careful trajectory design can ease the impact of the most probable failures on the mission goal. At the same time, a well-planned burn policy can considerably reduce the probability of fatal failure events.

1. Trajectory control policy and trajectory error analysis. Mission goals can be attained in more than one way for a given mission. This is particularly true of a continuously propelled, solar-electric mission.

Trajectory error analysis consists of identifying nonfatal (admissible) failure modes and providing alternate controls. In order to carry out such an analysis, a clear definition of mission success must be given. Once this is done, the impact of a failure can be evaluated and decisions can be made regarding the subsequent system control. In the event that the failure is severe enough to require a path modification, a path control policy is needed to modify the path to satisfy the mission goal in a unique manner. This policy will depend on the type of mission, but generally it can be as follows. The policy of control modification will be first to attain the final spacecraft state requirement (relative to the target) at the time closest to the nominal time. When this is impossible, it may resort to a secondary policy which will relax the final probe state constraints.

2. Thruster burn control policy. At every decision point of the mission operation process, the thrust-subsystem state $[U(t), \tau(t)]$ is given. Be it perfect or degraded by failures, the desired thrust program (that is, the varying power levels) must be matched according to a burn control policy. This policy is used to control the choice of thrusters, the switching time of the thrusters, and the duration of the thruster burn allocations at every phase of the mission.

Elaboration on such a policy may be made by closely following the result of the trajectory error analysis to enhance mission success. Simple models of the burn policy can be as follows. The number of burning

thrusters should be the minimum possible, as this avoids operation of the thrusters at low efficiency levels. The choice of thrusters to be on should not violate thruster array symmetry requirements and should attempt to maintain the smallest number of switching operations and distribute the load of burn evenly on all the available thrusters. The criterion for choosing a burn policy is its reliability. There are several different sources of failures, as will be discussed later in the section on hardware reliability. The least-switching and equal-burn policies discussed below are considered to give the highest reliability under such a reliability model.

Given a thrust program, the required total burn time T_B can be obtained simply by adding the product of the number of thrusters and the burn time for different phases of the mission (see Fig. 5). If T_i is the assigned burn time for the ith thruster, the reliability R of such a burn policy would be

$$R = r(T_1)\, r(T_2) \cdots r(T_N) \tag{2}$$

with the constraint

$$T_1 + T_2 + \cdots T_N = T_B \tag{3}$$

where

$r(T)$ = (PC + thruster) system reliability

N = Number of thrusters used

If the lifetime of the thrusters is very long and $r(T_i)$ are essentially of the exponential type,

$$r(T_i) = e^{-\lambda T_i} \tag{4}$$

then the reliability of performing the required burn

$$R = e^{-\lambda T_B} \tag{5}$$

is independent of the burn policy as long as the existing number of thrusters meets the minimum requirement. However, in reality, thruster life is of

finite duration and can be considerably shorter than the mission flight time. Because $r(T_i) \to 0$ as T_i approaches the lifetime, leading to complete failure, an arbitrary burn policy must be avoided. Since failure rates are monotonically increasing functions of elapsed burn time under the assumed reliability model, it can readily be proven that equal distribution of burn time to the existing thrusters would be the minimum risk policy.

Minimization of R with the constraint of (Eq. (3)) requires that

$$\frac{\dot{r}(T_1)}{r(T_1)} = \frac{\dot{r}(T_2)}{r(T_2)} \cdot \cdot \cdot \frac{\dot{r}(T_N)}{r(T_N)} = \text{minus hazard rates} \tag{6}$$

which can be satisfied if $T_1 = T_2 = \cdot \cdot \cdot T_N = T_B/N$. The above argument disregards the risks associated with thruster restart. In actual operation, it is perhaps more convenient to operate thrusters continuously as long as the operating condition is good and the switching of thrusters takes place only as a result of failures or as the number of thrusters burning is to be changed. Without sufficient spares, such a policy would have little chance to succeed in the most desirable mission mode. However, the probabilities of attaining the mission objectives in alternative modes could be great enough to be acceptable. This procedure is termed the "least-switching policy". In this study, the equal-burn policy is emphasized, where the consideration of equal-burn distribution is of primary importance and the least switching consideration is of secondary importance.

B. Hardware Risk Factors

1. Thruster power rating and number of thrusters. Once a nominal mission and the reference trajectory are chosen, the required power profile, which varies as a function of time, is determined. Since the thrust mode presupposes full utilization of solar panel output power, the thrust subsystem must be designed to operate with such a power history (power matching). The general practice of power matching is, first, to provide a number N of thrusters of given power rating (P_r) (power input to power conditioner) such that (NP_r) is at least equal to the maximum power yield of the solar panel during the entire mission. The variations in the power profile are matched by adjusting the number of engines in operation and, at the same time, relying on the ability of the engines to throttle in the range of about 2 to 1.

The engine power rating affects the mission reliability mainly through its impact on the possibilities of trajectory reshaping. The intuitive assumption that many smaller engines are more favorable than fewer larger ones (in that, following a failure (smaller power loss), the former leaves more chance of mission completion in alternative modes) is correct. Nevertheless, the thrust-subsystem specific mass increases as the power rating is decreased. This and the thruster array configuration design constraints should restrict the allowable value of P_r to a practical range.

Provision of spare thrusters always increases mission reliability. The required number of spares to attain a certain reliability depends on all other risk factors. Assuming, however, that all other risk factors remain the same, one can conduct risk analysis on all feasible ($N-P_r$) combinations. Prior to an actual subsystem design, such information is most desirable, as it will expedite the selection of a design point which is most cost-effective, compatible with design constraints, and deliver the needed success confidence level.

2. Power conditioner and thruster switching matrix. The use of switching mechanisms to allow interconnection of a power conditioner (PC) to many thrusters may add to system reliability. To include this factor in the analysis, in addition to the modeling of the switching logic, the switching mechanism reliability data must be given. Because this was beyond the scope of the study, the simulation of independent PC failures was not performed. One-to-one PC-thruster connections were assumed; thus the failure probabilities used represent the PC-plus-thruster unit.

3. Thruster array geometry. Because of spacecraft attitude stabilization requirements, the simultaneous operation of thrusters in some combinations is forbidden. The constraints reduce the possible alternatives in thruster burn in case of failures, and the burn strategy simulation must exclude such combinations.

4. Thrust subsystem reliability. The key constituents of reliability in the thrust-subsystem must be identified for a failure analysis. The mathematical models of failures must be established to allow a quantitative description of the failure probabilities. Systematic testing programs are needed to obtain actual failure distributions in the time domain and in the

operating environment extremes. At present, the data available are of a preliminary and speculative nature. However, these preliminary data can be used to carry out parametric studies wherein the parameters cover the entire possible range.

The key failure modes considered are:

(1) Thruster life. Thruster life is limited by grid wear-out or by depletion of the cathode emissive material.

(2) Thruster or power conditioner component failure. According to standard reliability engineering procedure, such failures can be considered to have a Poisson distribution.

(3) Thruster restart failure. The risks involved in restarting a thruster are modeled by using a binomial distribution.

(4) Delivery or infant failure. Conventional modeling of this type of failure can be made. However, in this study, it is assumed that the thrusters would be tested thoroughly and that this type of failure can be ignored.

Table 1 summarizes explicitly the mathematical models used. (See Ref. 4 for the standard reliability modeling.) A typical computer plot of the reliability curve R(t) is shown in Fig. 3.

IV. RISK PREDICTION METHOD

As introduced earlier in this section, the risk prediction method simulates countable discrete multistage processes and also calculates the corresponding probabilities.

This approach minimizes the labor of numerous trajectory computations by concentrating on a finite number of trajectory alternatives which can be used to approximate any of the actual alternative trajectories. The main purpose of the analysis is to investigate the mission feasibility and the probability of mission success. It is not mandatory to have very accurate trajectory profiles to conduct this type of study. In the following, a step-by-step description of computerized risk prediction and process simulation procedure is given.

Step 1. A finite number of trajectory points is systematically chosen to divide sequentially the entire mission into M different phases. The division can be based on the time interval during which the desirable number of thrusters that are turned on is constant. However, the size of a phase interval should not be too large. These time points constitute the decision times.

Step 2. At the beginning of each phase, the admissible failures are identified and alternative paths constructed. This method proceeds in a chronological order. As the stages progress, it is necessary to branch into a number of different paths, thus forming a trajectory tree. A summary of the resulting trajectory tree can be constructed in a graphical form, where correspondences between the thrust subsystem status (only the number of surviving thrusters) and the paths are shown. In general, the correspondence is one path to many thrust subsystem states. Besides, the only information important for the probability calculation is the power profile change along the alternate paths. This information is stored in the computer.

Step 3. Thruster reliability data are calculated by using assumed models, and the data are stored in a tabular form.

Step 4. The thruster burn is started in accordance with a burn policy and a nominal thrust program at the beginning of ith mission phase.

Step 5. A failure mode I_i, which may occur during the ith phase if step 4 were executed, is simulated. If there are N_i thrusters available at the end of the last phase, it is possible to have

$$\left(\sum_{j=1}^{N_i} C_j^{N_i} \right)$$

different modes of failures, where $C_j^{N_i}$ is a binominal coefficient. The probability of this I_ith failure mode is computed using the results of Step 3. Discard all events having less than 10^{-6} probability.

Step 6. If the failure mode I_i is not fatal, the thrust mode modification based on Step 2 is applied (i.e., path modification), the engine burn

allocation revised, and the ith phase completed. The probability of the ith phase completion

$$\left(P_{I_i}(i)\right)$$

in this revised mode is then computed.

No random number generating schemes are used to assign an exact time of failure. It is assumed that the impact of a failure occurring any time within the phase is approximately the same as if it were occurring at the beginning of the phase. Thus, revision of burn allocation always starts at the beginning of the phase. This gives conservative estimates.

Step 7. Proceed to (i+1)th phase: Steps 4 to 6 are repeated until the last phase of the mission is completed. The probability of mission completion with a failure history I (sequential failure modes I_i, I = 1, M constitute a failure history), is

$$P_I = \prod_{i=1}^{M} P_{I_i}(i)$$

Step 8. Steps 3 to 7 are repeated for all possible failure histories, giving a total success probability of

$$P = \sum_{I} P_I$$

The justification and advantage of the above procedure can be argued as follows:

(1) In the limit, where the number of phases chosen becomes infinitely large and the interval infinitely small, the method of prediction is mathematically exact.

(2) By a convenient choice of phases, an approximate trajectory prediction can be made, which in turn greatly reduces the labor of trajectory reoptimization.

(3) The inaccuracies in prediction made by the finite interval procedure can actually be measured only if one experiments with the size of the interval. This procedure is impractical from a computational point of view (at least, in the case of the Encke mission risk analysis used as an example in the next sections) because the required number of failure history simulations increases almost exponentially as the number of phases is increased. However, the estimate is on the pessimistic side, and it is believed that the error cannot be large; it is probably insignificant compared with whatever errors were being committed in the modeling of the hardware reliabilities.

V. 1980 ENCKE RENDEZVOUS MISSION RISK ANALYSIS

As an example of this risk assessment procedure and the type of information that can be generated by its application, an analysis was made of an Encke rendezvous mission for the 1980 opportunity.

A mission with the general mission profile shown in Table 2 was selected for analysis.

A. Hardware Risk Factors

1. Thruster power rating. This study assumes that the maximum allowable power input to a PC-plus-thruster system is 3.23 kW with a throttling ratio of 2 to 1. The 3.23-kW number is assigned to match the expected maximum solar array output power of 16.14 kW during the mission, using five thrusters. However, this number is compatible with a 30-cm thruster being considered at JPL.

2. Number of thrusters. Thrust subsystems with 5, 6, and 7 thrusters are analyzed in this study.

3. Symmetry requirements on thruster firing. Consider a 7-thruster system which has the geometrical configuration shown in Fig. 4. The simultaneous operation of combinations of thrusters which are prohibited is summarized in Table 3.

4. Hardware failure parameters. No firm data could be obtained regarding the reliability of the thrust subsystem. However, based on the

content of Ref. 5 (private communication from NASA Lewis Research Center), the following assumptions were made:

(1) Thruster life in the range of 300 to 450 days was assumed. In practice, thruster life is measured in terms of ampere-hours. In modeling the wearout failure, the independent parameter should be the elapsed burn time in ampere-hour units (defined as effective elapsed burn-time). At a fractional-power-level operation, such as in Phase VIII (see below), where a thruster is to operate at about the 50% level, the effective burn time should be 44 days instead of 88 days. The conversion of simple burn-time into effective burn-time was not carried out in this study.

(2) For thrusters, failure rates of $(6 - 10)/10^6$ h are assumed. For PCs, the failure rates are estimated to be about the same as for the thrusters. Allowing an error with a factor of 2, failure rates in the range $(6 - 50)/10^6$ h were used for the thrusters plus PCs.

(3) A somewhat arbitrary number of 10^{-5} was assigned for thruster restart failures.

B. Operational Mode Risk Factors

1. Definition of mission success. Three different classes of success are considered in this study:

(1) Class I, the selected mission mode. In this mode, rendezvous with Encke occurs at the desired rendezvous time of -47 days to T_P.

(2) Class II, a degraded but acceptable rendezvous mode. Here, the mission goals are considered attained if the spacecraft can achieve rendezvous with Encke at any time between -47 to -27 days to T_P. This also ensures that the heliocentric radius of the spacecraft is larger than 0.7 AU at encounter.

(3) Class III, including flybys, if relative velocities are less than 1 km/sec.

As explained in Section II, Class II and Class III goals are included to explore the effects of the trajectory control policy on the predicted risks.

2. Trajectory control policy and trajectory error analysis. At the onset of the selected mission, the thrust power level profile is expected to follow the curve given in Fig. 5. Even though this profile may change due to failures as the mission progresses, this power profile constitutes the basis for the thrust subsystem design and the power matching burn control of the first phase of the mission. Note the absence of a coast phase and the high power levels appearing at the initial and final phases of the mission. In accordance with Step 1 of the risk prediction method described in the previous section, the entire mission duration is divided into 15 different mission phases. This division of mission phases coincides with the times where the number of burning thrusters changes. The long phase of about 620 days in the middle where only one thruster needs to be burning is further divided into seven smaller phases for multistage simulation. The path control policy used to generate alternative paths, in case of severe failures, for the Class II goal is to attain a perfect rendezvous condition with minimum rendezvous time slippage from the Class I goal.

For the Class III success category, there are some difficulties in the calculations due to limitations existing in currently available low-thrust trajectory software. The results of trajectory error analysis as described are summarized in the trajectory tree shown in Fig. 6. There are seven different paths in this figure. These paths are considered to approximate adequately any of the actual paths the spacecraft will pursue following admissible failures. The straight lines between neighboring nodes represent one segment of the spacecraft path. Branching of the path appears as failures of different degrees occur.

3. Thruster burn control policy. Both the equal-burn policy and the least-switching policy were considered in this study. To illustrate the concept, the burn control expected for the selected mission can be planned as shown in Fig. 7. Also shown in Fig. 5 with the power profile is the minimum number of thrusters required at each phase of the mission, along with the expected average thruster burn allocation for thrust subsystems with 5-, 6-, or 7-thruster arrays.

C. Risk Prediction

An example of the computer output simulating a single failure process (failure history) and the corresponding probabilities as described in Steps 4 to 7 of the risk prediction method is given in Table 4. The assessed mission success probability is derived from a very large number (up to 10^6 cases) of such simulations.

D. Results and Conclusions

The predicted success probabilities for the 1980 Encke rendezvous mission are summarized in Table 5. These are shown as a function of thrust subsystem failure parameter sets (i.e., thruster life and failure rate) and mission class. Effects of symmetry requirements and the least-switching policy were examined for one set of hardware failure parameters. Conversion of the data of Table 5 into a constant risk-contour map (see Fig. 8) revealed some useful information regarding the hardware design requirements. The following conclusions were drawn from the data obtained.

1. Effects of hardware reliability on the thrust subsystem design. As assumed previously, if 3.23 kW were a convenient thruster power level for design, then the 5-thruster system would obviously not be satisfactory: it does not guarantee 90% reliability even when using very optimistic hardware-failure data. For 6-thruster and 7-thruster systems, constant-risk contours for the Class II mission goal are plotted on a failure parameter plane (Fig. 8). The shaded domain represents the currently assumed failure data bounds. If less than 1% risk is desired for a N = 6 or N = 7 system, the design effort must be made to shift the hardware failure data domain to the left of the 1% curve. Note the asymptotic behavior of constant-risk curves. As the thruster-life parameter increases, the constant-risk curve approaches asymptotically to a constant-failure-rate line. At the other extreme, the constant-risk curve tends to coincide with a constant-thruster-life line as the failure rate approaches zero. This implies that, with a fixed number of thrusters and a given failure rate, improvement in thruster life beyond a point does not contribute to the reduction of mission risks. For the same reason, given a fixed thruster life, design efforts beyond a point to reduce hardware failure rate is ineffective.

With the current design baseline, Fig. 8 indicates that thruster life is not the key risk factor in controlling the Encke mission if a 6- or 7-thruster system is desired. The low-risk contours are approaching the constant-failure-rate lines at the current thruster life expectancy. To reduce the mission risk, it is more effective and desirable to control the failure rate to less than the asymptotic value. For a 7-thruster system, the desirable 1% risk curve tends to approach the failure rate $\simeq 15$ line after a thruster life of above 500 days. Thus, unless one is fairly sure of controlling the failure rate to less than 15 per 10^6 h, a 7-thruster system cannot attain a 99% chance of success, even with very long-lasting thrusters. In this case, an 8-thruster system will be required, or the advantage of multichannel PC to thruster switching must be investigated. If a thruster failure rate of 6 and a PC failure rate of 7, as predicted by the hardware technicians, were reliable, then a 7-thruster system could be considered to be adequate because, by all indications, thrusters lasting 450 - 500 days are within reach with present technology.

2. Effects of symmetry requirements. In view of the conclusions reached above, only the 7-thruster system needs to be considered. Even though the data obtained are not exhaustive, it is expected that, within the current failure data domain, the symmetry constraint can degrade the mission reliability by no more than 1%.

3. Effects of trajectory design. The data in Table 5 show significantly greater success probabilities for the Class II mission goal as compared to the Class I goal, which means that a mission design which allows up to a 20-day encounter time delay helps to ease the mission risk considerably. This fact, in turn, eliminates the possibility of over-designing the thrust subsystem. The risk contour plots for the Class I mission goal shown in Fig. 9 illustrate this point. The confidence levels exhibited for a 7-thruster system appear similar to that of the 6-thruster system shown in Fig. 8. Thus, if the possibility of a Class II type of achievement were disregarded and the design point were chosen in the manner discussed in the previous paragraph, an 8-thruster system would have to be recommended. This is one thruster more than required. Since the main cause of the risk lies in the large random failure rates of the components which basically are difficult to control, it appears that it is much more effective to compensate

for the hardware unreliability by means of an over-designed trajectory rather than an over-designed thrust-subsystem. It is, therefore, recommended that future mission designs should consider risk aspects in the construction of the trajectory rather than adhering to the payload optimization procedure.

4. Class III mission goal. Consideration of the Class III mission goal and the chances of success have not been investigated in as much detail as the Class II mission goal. The main difficulty in analyzing this class of mission is in forming the trajectory tree. Because there is no software which will generate a minimum flyby velocity (V_{hp}) and the associated trajectory simultaneously, it is necessary to scan over many V_{hp}s until a possible minimum is reached, which requires many trajectory searches. In addition to the freedom in the choice of $V_{hp} < 1$ km/s, there is another degree of freedom, the encounter time (T_{end}) in establishing the failure-mode to alternate thrust-mode correspondence. This added degree of freedom in the choice of available trajectories demands another law (criterion) to single out one point in the acceptable (V_{hp} - T_{end}) domain and the corresponding thrust mode. In this particular study, where rendezvous mission is the main interest, no extra effort was made to solve the problem of the flyby-class goal in an exact manner. However, a preliminary study of the possibility of flyby missions ($V_{hp} < 1$ km/s) in case of severe failures was made. An arbitrarily selected, but valid, failure-to-flyby-mode correspondence was set up and the risks evaluated for a 5-thruster system. The results show that, for median failure parameters, the probability of success for the Class III mission goal is 94% compared with 87% for the Class II mission goal. This number indicates that uncertainties (2 - 3% risks) in the recommended 7-thruster system can be completely erased if the Class III mission goal is considered acceptable.

5. Effects of burn policy. As expected, the least-switching policy is inferior when compared to the equal-burn policy in achieving either Class I or Class II mission goals. This is particularly true for a Class I mission objective because thruster life is limited and only a limited number of thrusters are available. As the assumed wearout life becomes long and the number of available thrusters becomes large, normal failure dominates, and the risk becomes insensitive to the policy. Such appears to be the case

for the recommended 7-thruster system in achieving a Class II mission goal. For currently estimated failure data, the difference in predicted risk between the least-switching and the equal-burn policies is not expected to be more than 1 to 2% for the 7-thruster system.

VI. RECOMMENDATIONS

Wider application of this technique to other missions may be attempted to acquire a deeper understanding of the risk aspects of an SEP mission. Refinements to the method of risk prediction and the algorithm of failure-process simulations are most desirable. Further research in this area, with a better understanding and model of an actual SEP flight operation, may result in a more accurate semi-analytic approach to the problem, which is most vital for the support of SEP missions.

REFERENCES

1. Russell, K. J., Seliger, R. L., "Electric Propulsion Design Optimization Methodology," Journal of Spacecraft and Rockets, Vol III, No. 2, Feb. 1970, p. 164.

2. Guttman, C. H. et al., "The Solar Electric Propulsion Stage Concept For High Energy Missions," AIAA Paper No. 72-465, American Institute of Astronautics and Aeronautics, April 1972.

3. Kizner, W., "An N Thruster Reliability Problem for Electric Propulsion," JPL Space Programs Summary 37-60, Vol. III, Dec. 1969, p. 223-226.

4. Myers, R. H., Wong, K. L., Gordy, H. M., Reliability Engineering for Electronic Systems, John Wiley and Sons, Inc., 1964.

5. Paul Reider, personal communication, Reliability Data and Failure Modes of 30 cm Thrusters, NASA Lewis Research Center, March 27, 1972.

Table 1. Failure modes and mathematical models

Failure Type	Failure Distribution Model	Reliability
Delivery (infant)	Binomial	s
Start-up	Binomial	q
Thruster, normal operating	Exponential	$R_1(t) = e^{-\lambda t}$
Thruster wear-out	Log-normal	$R_2(t) = \int_t^\infty \left[\frac{1}{\sigma\sqrt{2\pi}\,\tau} e^{-(\lg \tau - \mu)^2/2\sigma^2} \right] d\tau$ $R(t) = R_1(t)\, R_2(t)$ $T = e^{\mu + \sigma^2/2}$ $\Delta T = \sqrt{e^{2\mu + 2\sigma^2} - e^{2\mu + \sigma^2}}$
Power conditioner	Same as thruster	Since one to one PC-thruster switching is assumed, it is not necessary to model the PC failure separately. For PC + thruster system, the failure rates are additive, and the wear-out life should be the shorter one of the two components.

Note:
t = Elapsed thruster burn time
R = Total reliability
λ = Thruster failure rates
T = Thruster wear-out life (mean)
ΔT = Thruster wear-out life (standard deviation)

It is assumed that all thrusters have identical failure statistics and mutually independent failures.

Table 2. Characteristics of an Encke rendezvous mission

Event	Characteristics
Launch date	March 16, 1978
Arrival date	October 21, 1980 (-47 days to T_P*)
Solar panel size	P_o = 16.6 kW
Housekeeping power	P_A = 0.6 kW
Specific impulse	I_{SP} = 3000 sec
Injected mass	M_o = 1630 kg
Injection C_3	C_3 = 54.2 $(km/sec)^2$
Nominal final mass	M_f = 1163 kg
Propellant mass	M_p = 457 kg

*T_P = Time of Encke perihelion

Table 3. Forbidden thruster combinations

Number of Thrusters to be Fired	Forbidden Combinations
5	None
4	2347, 3457, 4567, 1567, 1267, 1237, 2467, 1357
3	237, 347, 457, 567, 167, 127, 247, 357, 467, 157, 267, 137, 234, 345, 456, 156, 123, 346, 135
2	25, 36, 47*
1	None

*Allowed combinations

For six-thruster system, thruster ⑦ is removed.

For five-thruster system, ② and ⑤ is removed.

Forbidden combinations for six-thruster system and five-thruster system can be inferred from the above table.

Table 4. A computer output for a failure process simulation and the associated probability

Phase Number	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV
Thrust Subsystem State History	*7	7	7	7	7	6	6	6	5	5	5	4	4	4	4
						Burn-Control History (Equal-Burn Policy)									
Thruster 1	**48	77	118	211	–	–	–	–	x	x	x	x	x	x	211
Thruster 2	48	77	118	211	–	–	–	–	–	–	–	–	239	253	260
Thruster 3	48	77	118	–	206	–	–	–	–	–	–	–	234	248	255
Thruster 4	48	77	–	–	–	x	x	x	x	x	x	x	x	x	77
Thruster 5	48	–	–	–	–	136	–	224	–	–	–	299	–	313	319
Thruster 6	0	–	–	–	–	–	88	–	176	–	–	x	x	x	176
Thruster 7	0	–	–	–	–	–	–	–	–	88	176	251	279	293	300
Probabilities of Success	0.966	0.983	0.982	0.974	0.987	0.0124	0.987	0.987	0.0126	0.987	0.987	0.0105	0.988	0.991	0.996

Note: Life = 450 ±50 days; Failure rates = $6/10^6$ hr; Restart risk = 10^{-5}

P_I (Probability of the failure process) = 0.137×10^{-5}

* Number of surviving engines.
** Elapsed burn time of the thruster at the end of the phase.
x Thruster failed.
– Thruster off.

Table 5. Probability of success for a 1980 Encke rendezvous mission

N	Life (days)→	450 ± 50			400 ± 50			350 ± 50			300 ± 50		
	Failure Rate ($\lambda/10^6$ hr)→	6	10	50	6	10	50	6	10	50	6	10	50
5	Class I	78.2 *77.8 ** 0.0	67.1 *66.7 ** 0.0	14.4 *14.3 ** 0.0	59.1	50.6	10.9	12.1	10.4	2.2	0.22	0.19	0.04
	Class II	93.5 *87.7 **81.0	87.7 *80.8 **71.0	39.9 *28.1 **18.9	85.0	77.5	27.3	42.0	36.8	9.61	1.92	1.71	0.40
6	Class I	97.5 *96.6 ** 8.7	93.9 *92.6 ** 7.5	41.5 *40.2 ** 1.6	95.2	90.7	38.2	80.3	72.6	23.4	23.5	20.4	4.9
	Class II	99.6 *98.9 **98.2	98.9 *97.3 **95.6	73.3 *61.4 **51.3	98.9	97.5	62.6	93.4	88.7	41.7	47.3	42.0	12.3
7	Class I	99.8 *99.5 **84.7	99.2 *98.5 **75.7	67.8 *64.3 **22.9	99.6	98.8	66.1	98.1	95.8	54.5	81.1	74.5	27.9
	Class II	99.9 *99.7 **99.8	99.8 *99.2 **99.5	89.5 75.6 **78.0	99.8	99.5	84.1	99.1	98.1	71.3	92.0	87.1	42.5

*Success probability with symmetry maintained in the thruster burns.
**Success probability using least-switching policy.

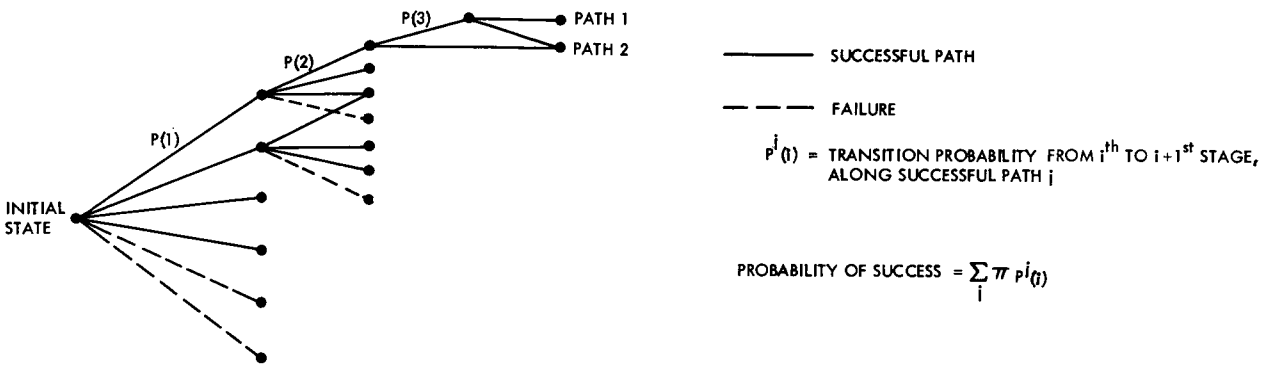


Fig. 1. Probability tree for mission operational process

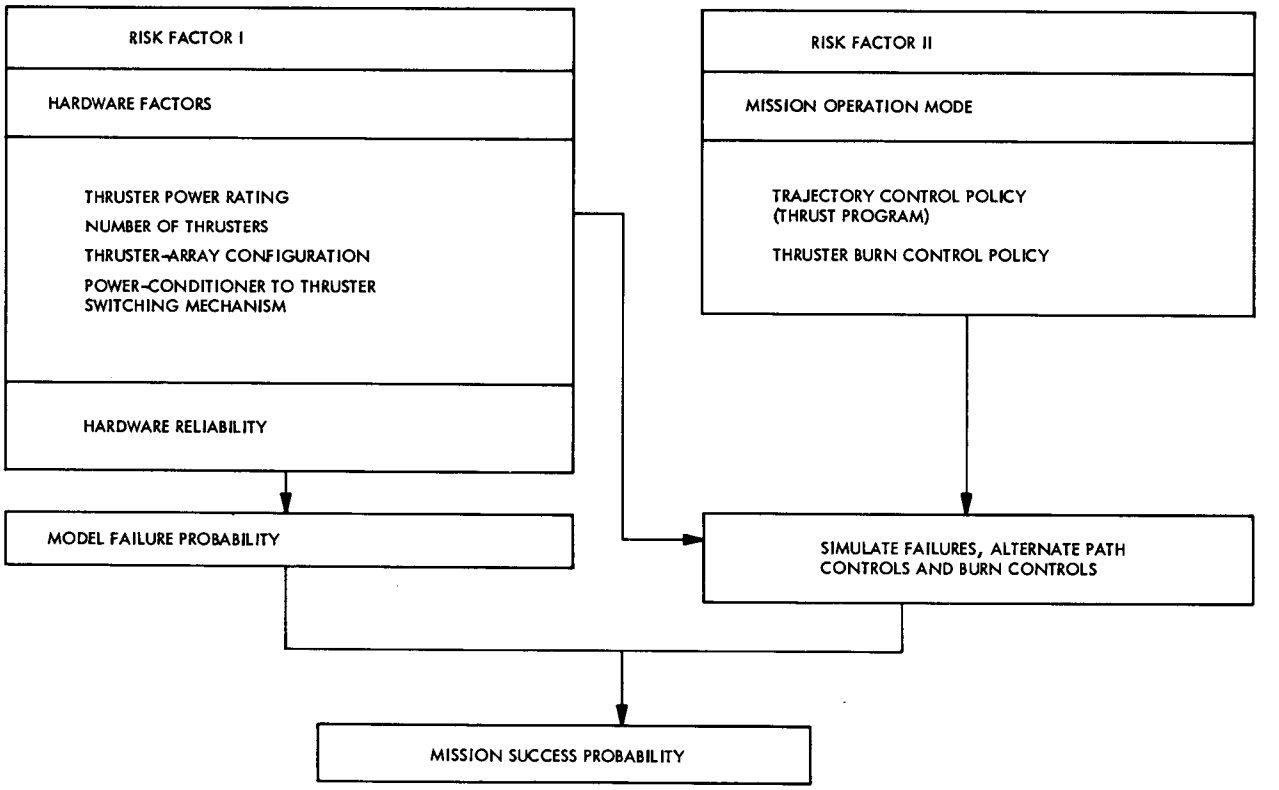


Fig. 2. Risk factors and risk assessment

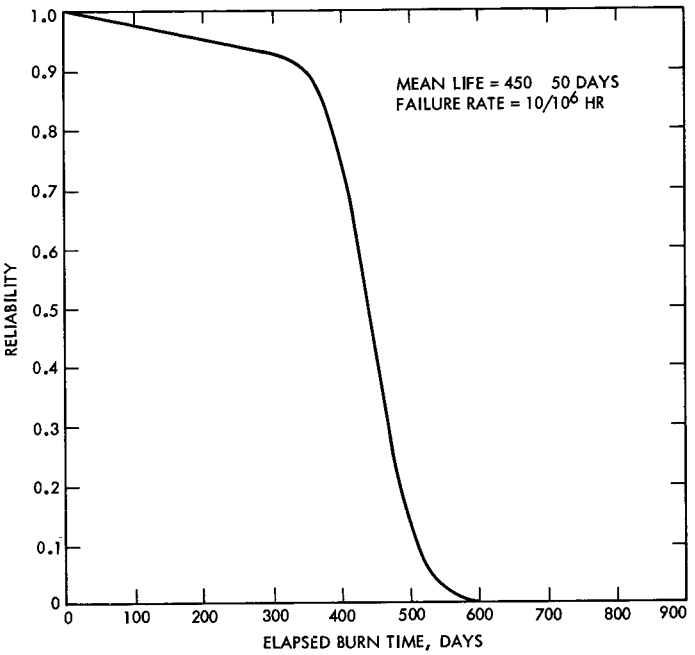


Fig. 3. An example of a reliability curve

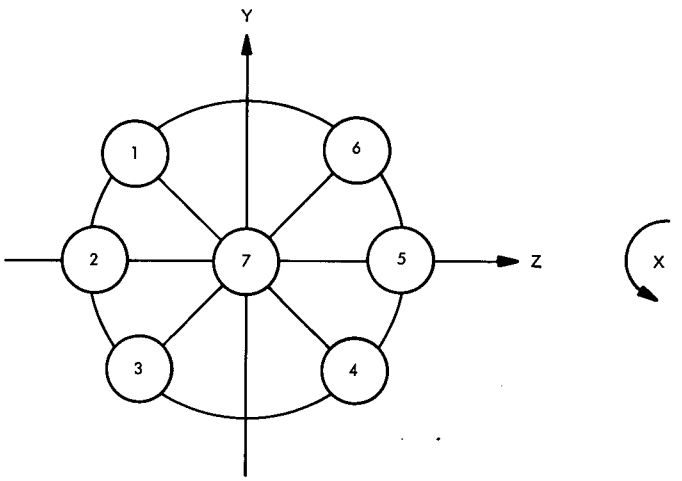


Fig. 4. Geometric configuration of 7-thruster system

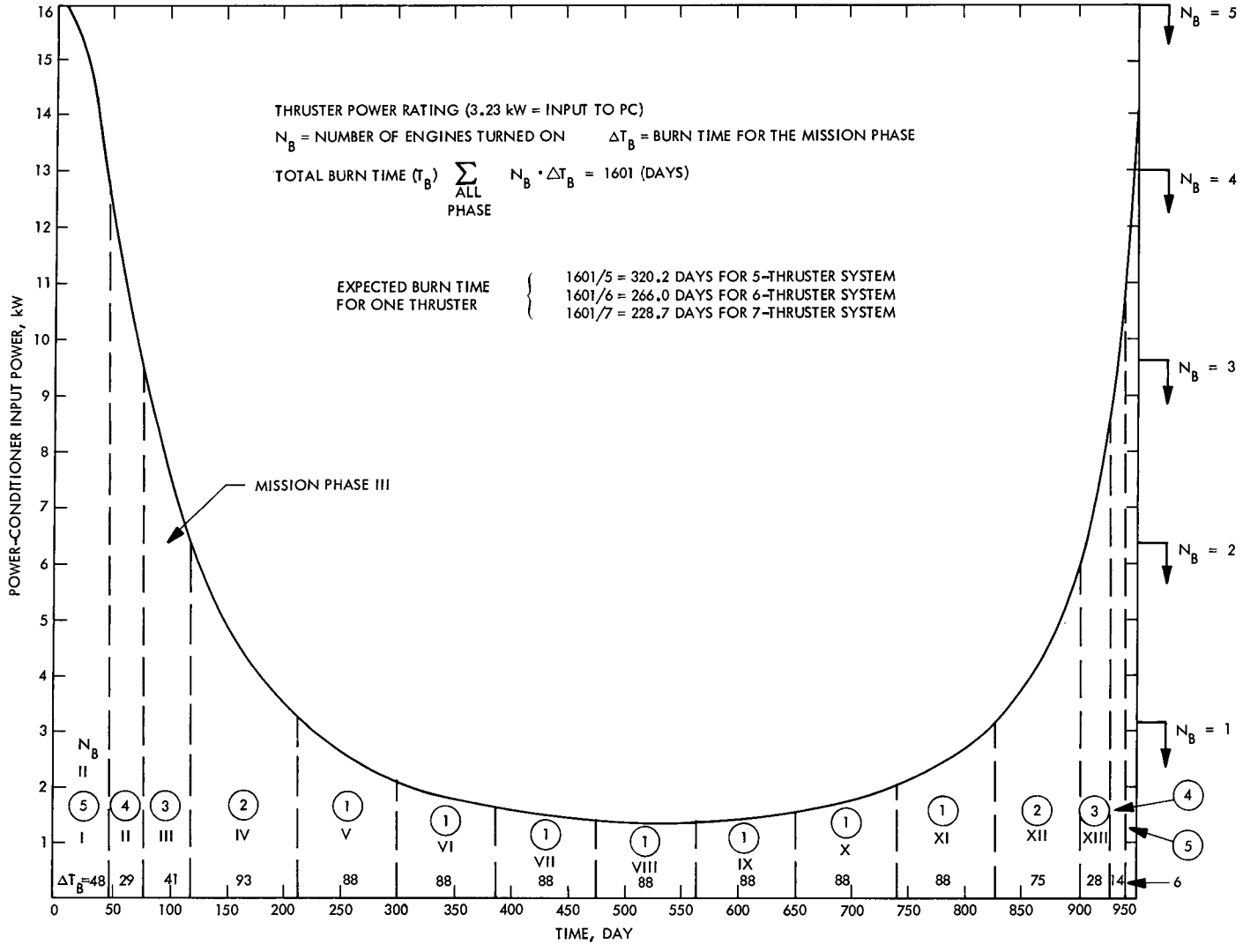
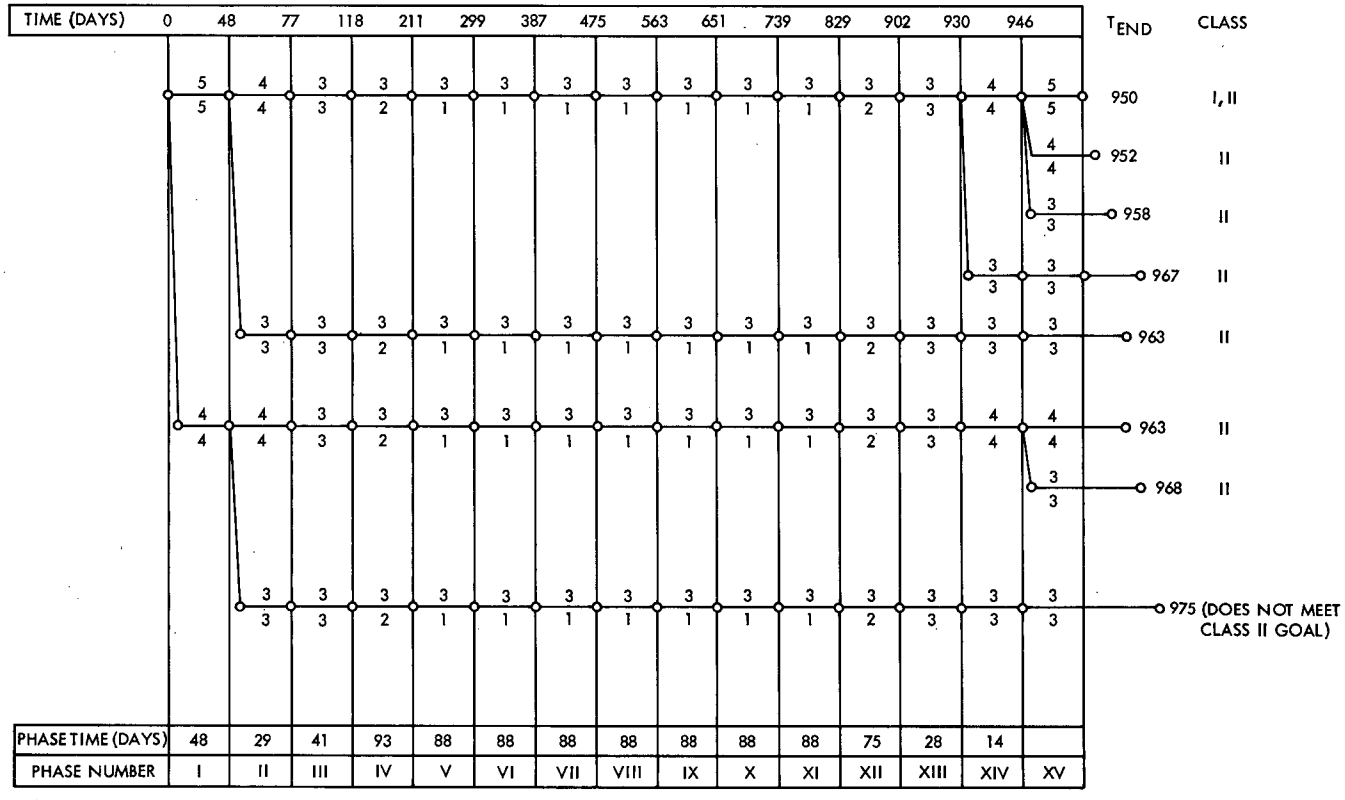
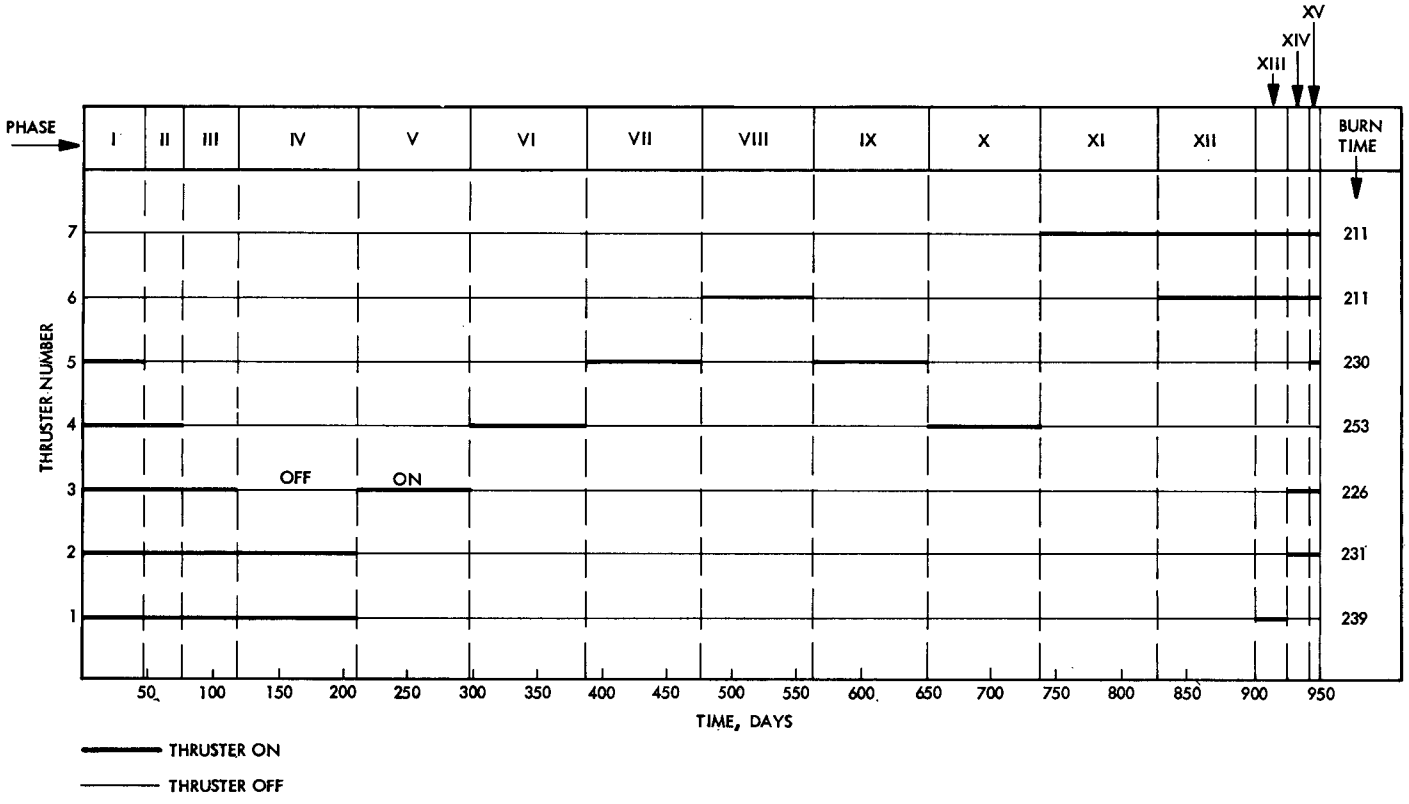


Fig. 5. Power profile, 1980 Encke rendezvous mission



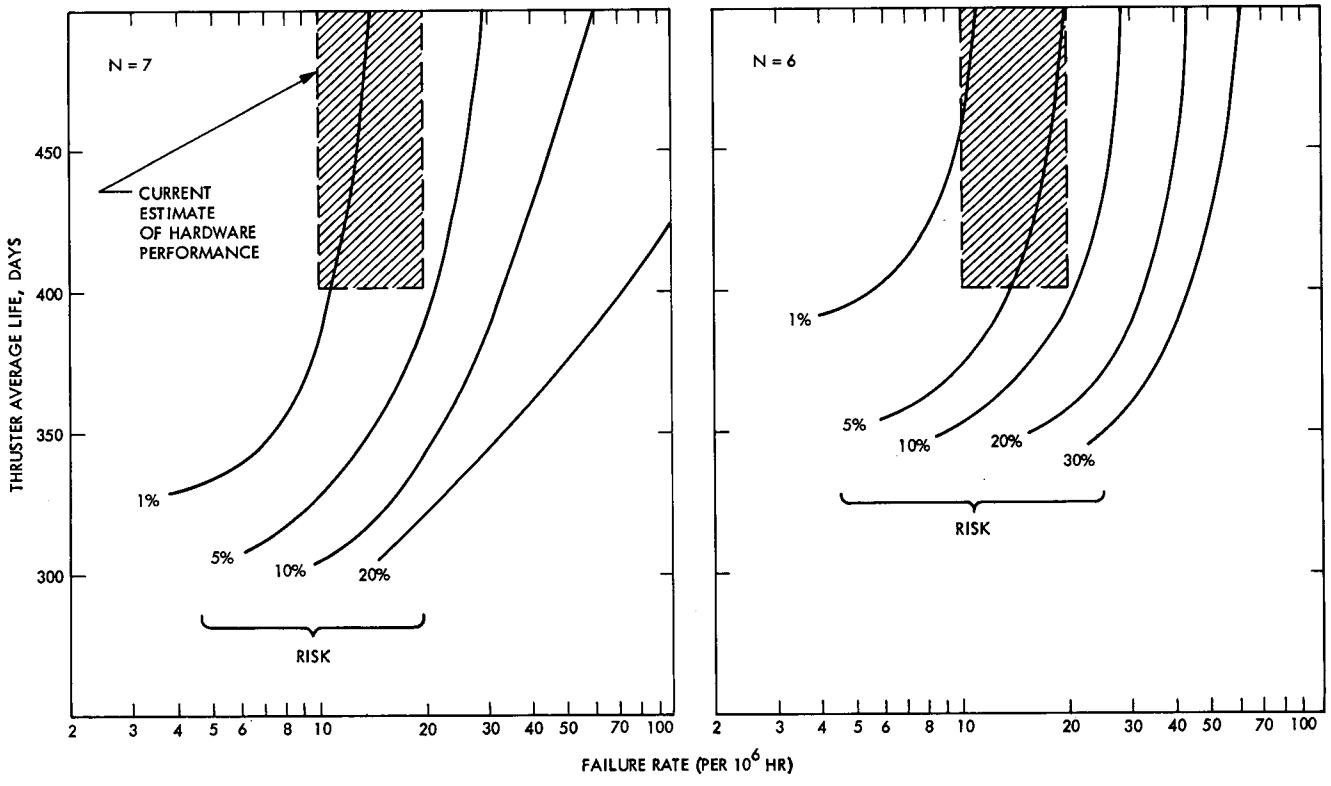
NOTE: NUMBERS ABOVE THE PATH o-o INDICATE THE MINIMUM NUMBER OF SURVIVING THRUSTERS NECESSARY TO BE ON THE PATH TO ACCOMPLISH THE MISSION.
NUMBER UNDER THE LINES INDICATES THE ACTUAL NUMBER OF THRUSTERS BEING USED FOR THE PHASE.

Fig. 6. Admissible trajectory alternatives (trajectory tree)



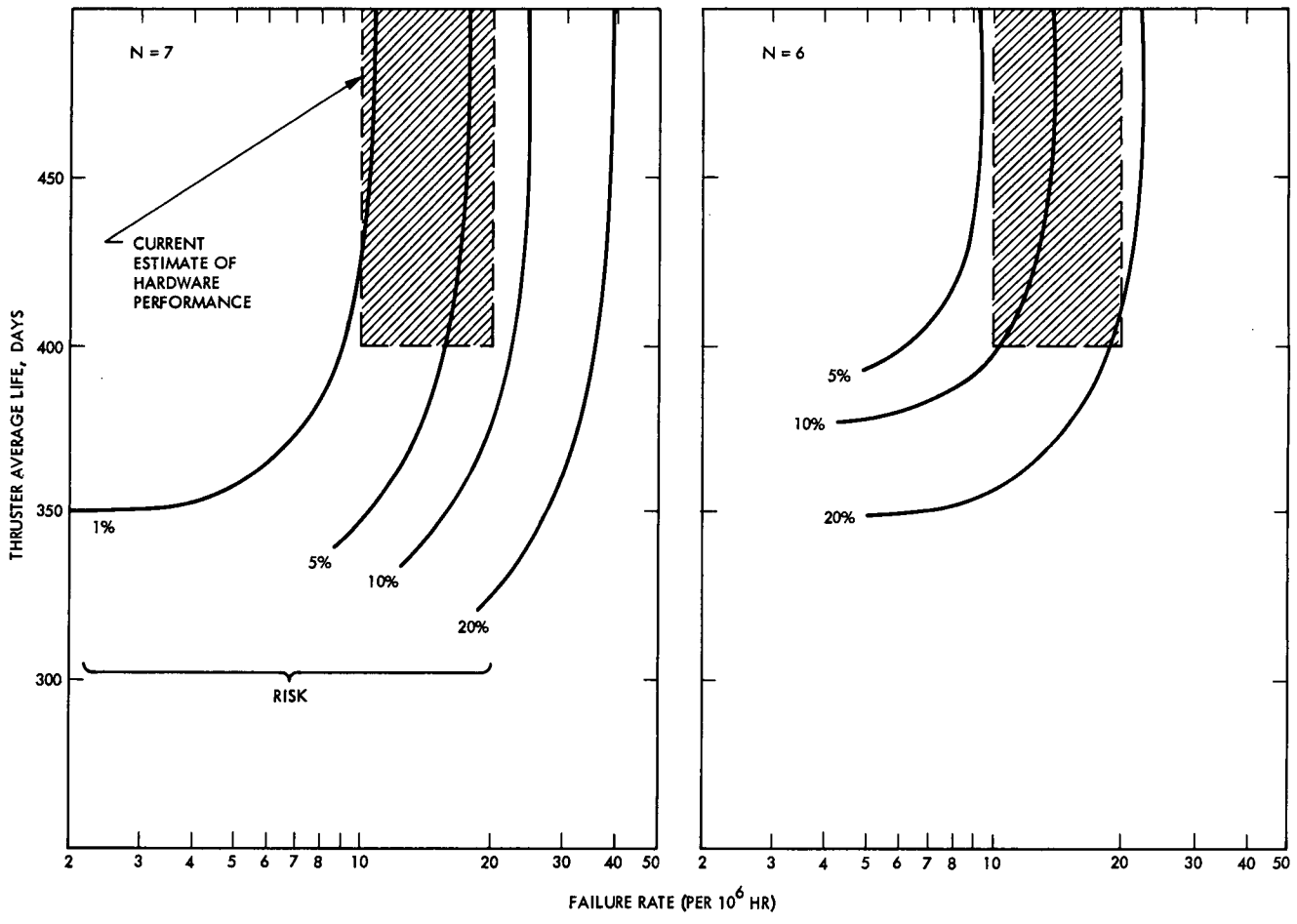
NOTE: THIS BURN SEQUENCE IS PRODUCED TO MATCH THE POWER PROFILE USING A 3.23 kW, SEVEN-THRUSTER SYSTEM. THE DEVIATION FROM EXACT, EQUAL BURN-TIME AT THE END IS CAUSED BY THE PARTICULAR WAYS IN WHICH THE MISSION PHASES WERE DIVIDED.

Fig. 7. Example of an equal-burn control policy



NOTE: CLASS II MISSION GOAL
N = NUMBER OF THRUSTERS
FAILURE RATES INDICATED ARE CAUSED BY PC PLUS THRUSTER

Fig. 8. Constant-risk contour map for 1980 Encke rendezvous mission, Class II mission goal



NOTE: CLASS II MISSION GOAL
N = NUMBER OF THRUSTERS
FAILURE RATES INDICATED ARE CAUSED BY PC PLUS THRUSTER

Fig. 9. Constant-risk contour map for 1980 Encke rendezvous mission, Class I mission goal

NASA – JPL – Coml., L.A., Calif.